arcserve
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Datenresilienz: Die rasante Zunahme von DNS-Angriffen erfordert neue Ansätze für die Cyberabwehr

Von Sven Richter, Marketing Manager DACH bei Arcserve

Zwischen März 2022 und März 2023 sind laut einer aktuellen Studie weltweit 66 Prozent der Unternehmen Opfer von Ransomware-Angriffen geworden. Viele dieser Vorfälle betrafen einen DNS-Angriff (Domain Name System), denn jedes DNS hat Schwachstellen.

Angreifer haben gleich mehrere Möglichkeiten, diese Schwachstellen auszunutzen. Eine bei Cyberkriminellen beliebte Methode ist ein „DNS-Flood". Dabei handelt es sich um einen verteilten Denial-of-Service-Angriff, der einen anvisierten DNS-Server überlastet. DNS-Angriffe können schwere Schäden anrichten: Sie stören Online-Dienste und geben Angreifern die Möglichkeit, das entstandene Chaos für weitere bösartige Aktivitäten zu nutzen, beispielsweise durch das Einschleusen von Ransomware zur Verschlüsselung wichtiger Daten.

Cyberkriminelle nutzen auch Fehlkonfigurationen in der DNS-Infrastruktur als Einfallstor für Ransomware-Angriffe, um unbefugten Zugriff auf das Netzwerk eines Unternehmens zu erhalten und nach dem Eindringen Ransomware zu verbreiten. Weiterhin können Hacker etwa auch das DNS-System nutzen, um ihre Opfer von häufig besuchten Webseiten wegzulenken und sie auf gefälschte aber legitim erscheinende Seiten zu leiten. Diese gefälschten Webseiten verleiten die Opfer dazu, ihre Anmeldedaten einzugeben oder unbemerkt bösartige Dateien herunterzuladen. Die Angabe von persönlichen Daten können Angreifer verwenden, sich innerhalb des Netzwerks zu bewegen oder eine Ransomware zu übermitteln.

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Zero Trust für mehr Datensicherheit

Da Ransomware immer ausgefeilter wird und DNS-Angriffe immer häufiger auftreten, versuchen Unternehmen, sich durch innovative Ansätze und Technologien zu schützen und so die Integrität und Sicherheit ihrer Sicherungssysteme zu erhöhen. Dazu gehört auch der „Zero Trust"-Ansatz. Dabei handelt es sich nicht um eine einzelne Technologie; es ist eine Verschmelzung von Richtlinien, bewährten Verfahren und verfügbaren Produkten. Zero Trust zielt darauf ab, eine Umgebung zu schaffen, die umfassenden Schutz vor potenziellen Bedrohungen bietet.

Ein Zero-Trust-Ansatz verbessert die Integrität und Sicherheit von Backup-Systemen, indem er die Art und Weise, wie Unternehmen über Netzwerksicherheit denken, grundlegend ändert. In einem herkömmlichen Sicherheitsmodell hat ein Benutzer oder System, sobald er Zugang zu einem Netzwerk erhält, oft weitreichende Zugriffsrechte - auch auf Backup-Systeme. Bei Zero Trust vertraut ein Unternehmen jedoch niemandem und setzt die Sicherheit auf jeder Ebene durch, auch bei Backup-Systemen.

Zero Trust folgt dem Prinzip der geringsten Privilegien, d. h. das Unternehmen gewährt Benutzern oder Systemen nur den Mindestzugang, der für die Ausführung ihrer spezifischen Aufgaben erforderlich ist. Im Zusammenhang mit Sicherungssystemen gewährleistet dieses Prinzip, dass nur befugte Personen und Prozesse Zugriff auf Sicherungsdaten haben, was das Risiko eines unbefugten Zugriffs und von Datenverletzungen verringert.

Folgen Sie Arcserve auf LinkedIn oder X und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Über Arcserve

Arcserve gehört weltweit zu den Top-5-Herstellern von Datensicherungslösungen und bietet als Anbieter von Unified Data Resilience Lösungen eine einheitliche Plattform für die Ausfallsicherheit von Daten an. Das Unternehmen stellt das breiteste Spektrum an Best-in-Class-Lösungen für die Verwaltung, den Schutz und die Wiederherstellung aller Datenumgebungen zur Verfügung. Die Lösungen von Arcserve eignen sich für KMUs und Großunternehmen, unabhängig von deren Standort und der Komplexität der Infrastruktur. Sie beseitigen die Komplexität und bieten gleichzeitig erstklassigen, kosteneffizienten, flexiblen und massiv skalierbaren Datenschutz und Sicherheit für alle Datenumgebungen. Dazu gehören On-Prem-, Off-Prem- (einschließlich DRaaS, BaaS und Cloud-to-Cloud), hyperkonvergente und Edge-Infrastrukturen. Dank der vier Jahrzehnte langen Erfahrung des Unternehmens mit preisgekrönten IP-Lösungen und der kontinuierlichen Konzentration auf Innovation können Partner und Kunden, darunter MSPs, VARs, LARs und Endbenutzer, sicher sein, dass sie den schnellsten Weg zu Daten-Workloads und -Infrastrukturen der nächsten Generation finden. Arcserve ist ein zu 100 Prozent channelorientiertes Unternehmen, das in über 150 Ländern vertreten ist und mit 19.000 Vertriebspartnern die kritischen Datenbestände von 235.000 Kunden schützt. Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf X oder LinkedIn.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de